ВЗЛОМ ДЛЯ НАЧИНАЮЩИХ

Где учиться пентесту. Обзор площадок для практики навыков этичного хакера

snovvcrash , только что  0  981 Добавить в закладки



Мобильная версия статьи

В этой статье мы выясним, какие площадки позволяют оттачивать мастерство взлома и ценятся специалистами по безопасности. Они позволяют этичным хакерам быть этичными до последнего, при этом не терять хватку, регулярно практиковаться со свежими уязвимостями и оставаться в рамках закона.

Сфера ИТ развивается семимильными шагами, компьютеры проникают в жизнь все

глубже, цифровые системы становятся более комплексными, а соответственно растет и поверхность атак. Это в свою очередь рождает спрос на специалистов по безопасности, в том числе — этичных хакеров.



WWW

Подробнее о профессии (или даже профессиях) этичного хакера читай в колонках Юрия Гольцева и Дениса Макрушина. Начать можешь с материала «Этичный взлом по шагам», который дает неплохое представление о том, чем и как занимается пентестер в белой шляпе.

Этичный хакер должен отлично разбираться во всей специфике темной стороны: если ты знаешь, как сломать, и поддерживаешь эти знания в актуальном состоянии, то сможешь давать и рекомендации по защите. В общем, главное здесь — практика, но как ей заниматься, не нарушая закон?

На заре нулевых многие энтузиасты кибербезопасности становились преступниками, хотя часто преступление заключалось лишь в любопытстве. Собственно, в «Хакере» то и дело можно было встретить рассказы о взломах реальных систем, написанные от первого лица.

Дело в том, что тогда альтернатив не было, а любопытства было хоть отбавляй. Но так не могло продолжаться долго. Времена изменились, и хакерам пришлось найти способы совершенствовать навыки наступательной безопасности легально. Сегодня существует ряд платформ, где всем желающим дают возможность попрактиковаться без риска попасть под тяжелую руку закона.



INFO

В этой статье внимание сосредоточено на относительно бесплатных лабораториях,

которые не требуют покупку подписки в обязательном порядке для доступа к своей инфраструктуре. Из платных аналогов, предоставляющих своим клиентам помимо всего прочего расширенные методические материалы, можно выделить Virtual Hacking Labs и PentesterLab Pro, схожие с курсом PWK.

Структура ресурсов

Есть несколько направлений, которых может придерживаться тот или иной ресурс, предлагающий практику пентеста. Обычно все их можно отнести к одному из трех больших разделов.

1. **CTF-таски** — всем хорошо известный Capture the Flag, который представляет собой отдельные задачи по определенной тематике. Обычно присутствуют такие категории, как Reverse, Exploit (или PWN), Web, Crypto, Stego, Forensics, OSINT и Misc. Чуть реже к ним добавляется PPC (спортивное программирование). Процесс выполнения такой задачи достаточно прямолинеен: загружаешь файлы, входящие в состав таска, к себе на машину, находишь флаг, вводишь его на ресурсе и получаешь свою награду.
2. **Уязвимые виртуальные машины** — более приближенное к реальной жизни испытание, которое заключается во взломе заведомо уязвимого хоста. Конечная цель — получение контроля над привилегированным аккаунтом системы. Доказательством окончательного захвата машины обычно служит демонстрация возможности чтения файлов (также содержащих своеобразный «флаг»), доступных пользователям с соответствующими привилегиями. Процесс прохождения такой виртуальной машины разнится в зависимости от устройства самой площадки, на которой обитает уязвимый хост: это могут быть как «живые» хосты, которые в текущий момент непосредственно находятся в сети на серверах площадки (онлайн-лаборатории), либо загружаемые образы для самостоятельного запуска в виртуальной среде.
3. **Виртуальные локальные сети** — как правило, виртуальные леса Active Directory, где от участников требуется захватить контроллер и закрепиться в сети. В ходе прохождения могут использоваться самые разные способы для продвижения по инфраструктуре: от конкурентной разведки и фишинга до эксплуатации 0-day уязвимостей. Сложность выполнения таких задач сопоставима с реальными кейсами, а зачастую даже превосходит их. Доступ к лабораториям такого типа обычно платный, а их услуги могут быть

максимально полезны людям, готовящимся к профессиональным сертификациям типа OSCP.

Для поддержания энтузиазма безопасников, которые пришли на такие ресурсы, владельцы часто предлагают им бонусы за прохождение каждого из вида заданий, которые могут выражаться в «плюсиках к карме», которая видна в профиле игрока и в «Зале славы». Место в таком топе потом может стать хорошим подспорьем на собеседовании.

Посмотрим поближе на наиболее крупные и известные площадки, где ты сможешь побаловать своего внутреннего хакера.

Hack The Box

Hack The Box (или HTB) — мой любимый ресурс, который позволяет оттачивать искусство тестирования на проникновение и по совместительству, пожалуй, одна из самый масштабных платформ, где на текущий момент доступно 127 уязвимых машин, 65 Task Based CTF-задач и несколько видов хардкорных виртуальных лесов AD. То есть, как ты уже понял, здесь есть все описанные выше области.

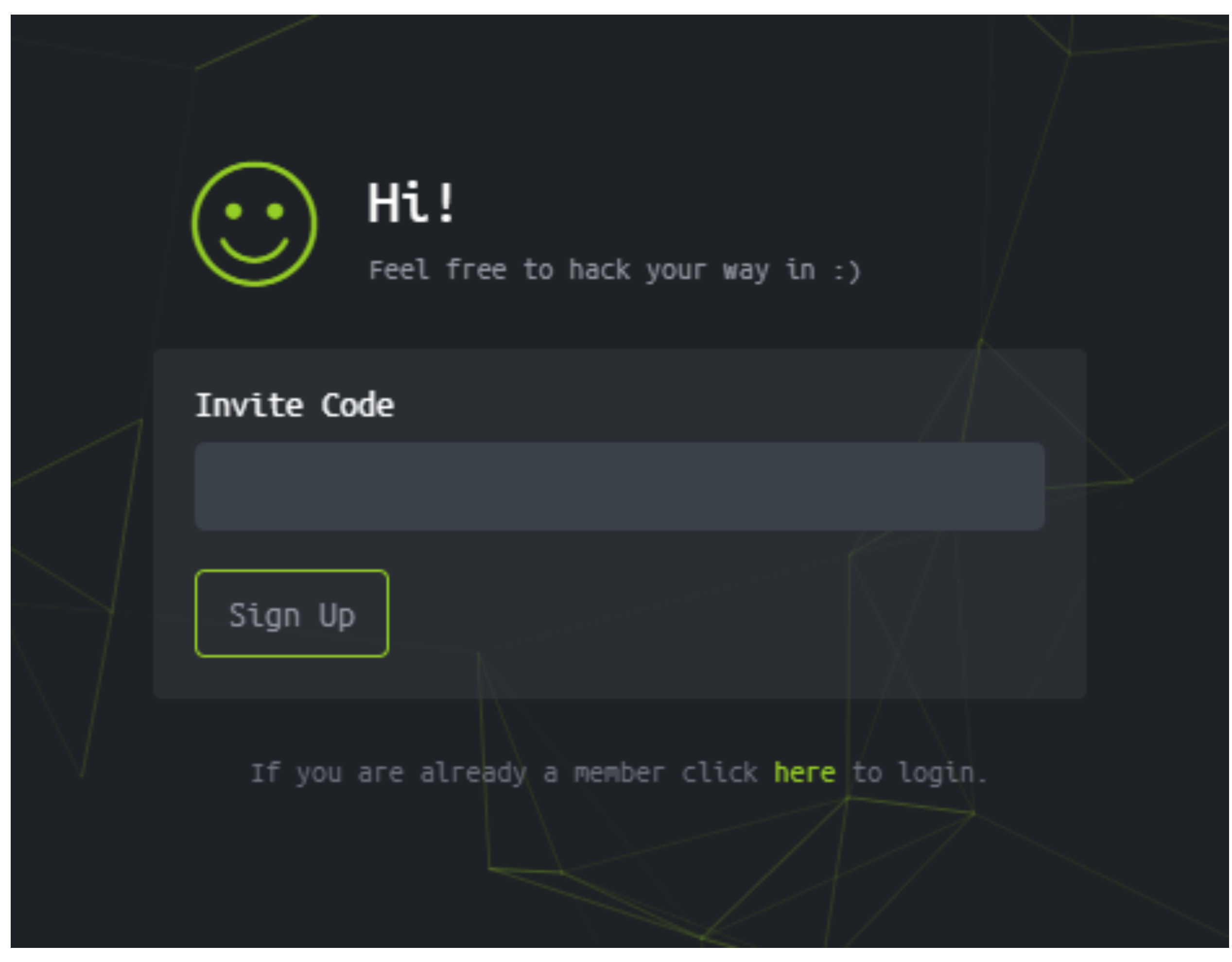


Hack The Box

За несколько прошлых лет Hack The Box стал максимально популярен среди исследователей безопасности всех мастей: он отличается удобным веб-интерфейсом для управления активными инстансами виртуалок, отзывчивой техподдержкой и, что важнее всего, постоянно обновляющемся списком уязвимых хостов.

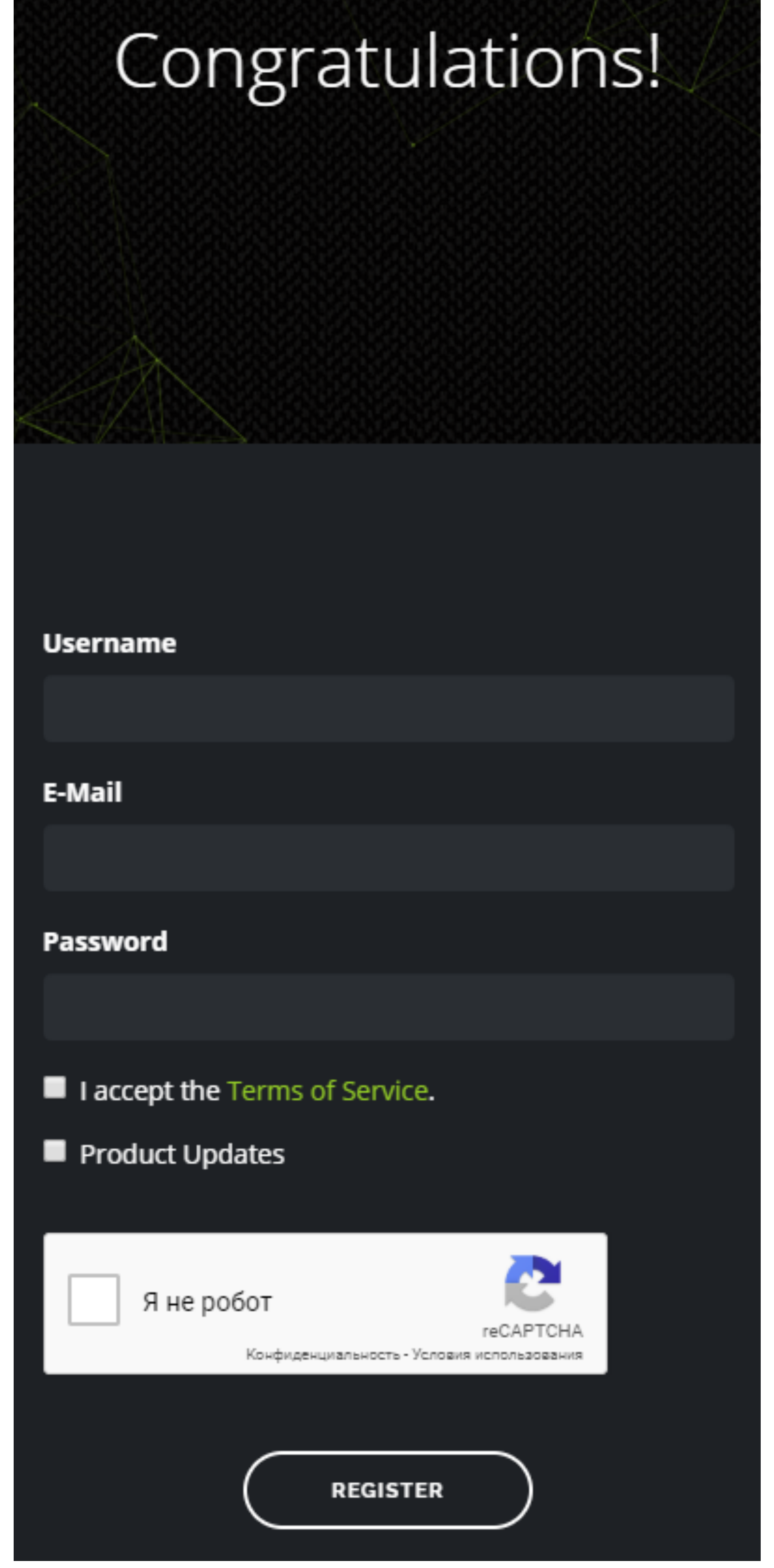
График выхода новой машины «в онлайн» очень прост: каждую неделю релизится новая тачка и становится доступной для взлома всем зарегистрированным на ресурсе игрокам; в то же время одна из машин, которая «висела» в онлайне до этого момента, уходит в пул отозванных машин. Всего одновременно в онлайне находится 20 машин... Но это только на бесплатном сервере. При оформлении VIP-подписки (£10/месяц или £100/год) ты сможешь самостоятельно вытягивать любой «устаревший» хост из пула в онлайн на выделенном сервере и проводить свои тесты. Также вместе с этой суперспособностью тебе откроется доступ к официальным прохождениям в формате PDF, которые составляют сами сотрудники ресурса.

Регистрация на Hack The Box предполагает решение тривиального веб-таска для получения кода на приглашение, поэтому я всегда условно считал этот ресурс полузакрытым. Почему условно? Потому что таск и правда элементарный, и в свое время я даже писал однострочник для генерации очередного инвайта. Разбирать сам процесс в рамках этой статьи не будем, поскольку невежливо будет раскрывать все подробности решения и обесценивать работу команды HTB. Тем не менее, гайдов в сети предостаточно.



hackthebox.eu/invite

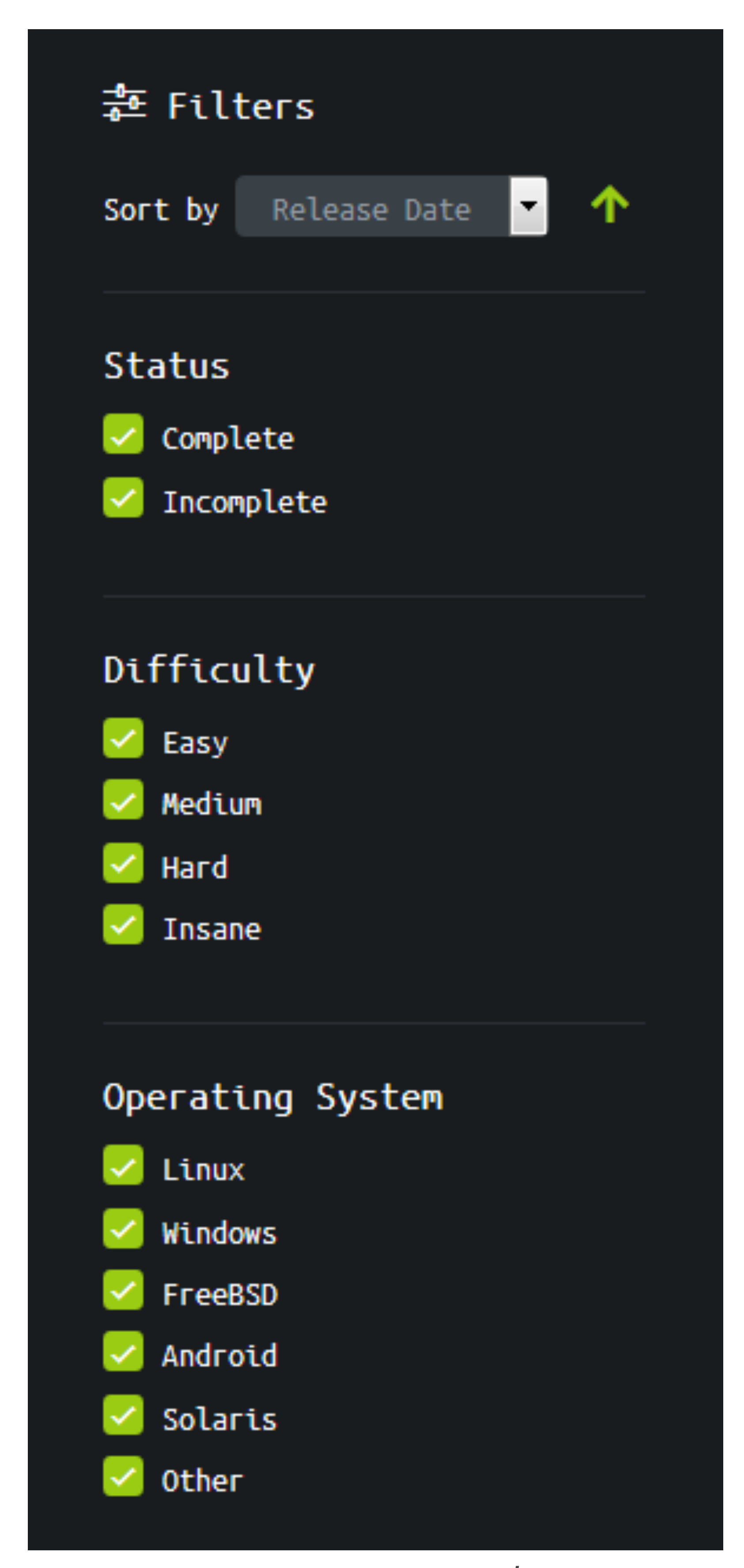
Однако, что меня удивило в процессе написания этой статьи, так это то, что ограничение на регистрацию, оказывается, легко обходится простым переходом на страничку регистрации. Не знаю, баг это или фича, и было ли так изначально, но факт остается фактом — сейчас это работает.



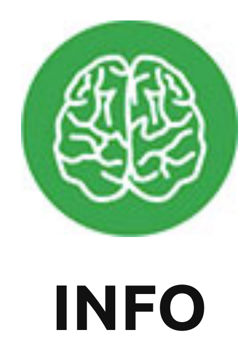
hackthebox.eu/register

Порог вхождения на эту платформу я бы оценил как средний: несмотря на то, что большую часть активных инстансов составляют виртуальные машины высокой сложности, на сайте можно найти и простые машины, рекомендуемые для прохождения начинающим свой путь специалистам. Гибкая система фильтров позволит тебе

подобрать машину на свой вкус.



Фильтрация списка существующих ВМ



INFO

«Хакер» уже публиковал несколько прохождений виртуалок с Hack The Box:

Укрощение Kerberos. Захватываем Active Directory на виртуальной машине с

HackTheBox
Великий пакостник. Пробираемся через дебри IPv6 к root-флагу виртуалки с Hack The Box
Полет в стратосферу. Ломаем Struts через Action-приложение и мастерим Forward Shell
Неправильный CTF. Одноразовые пароли, буйство LDAP-инъекций и трюки с архиватором 7z

Стоит заметить, что Hack The Box пользуется услугами DigitalOcean для развертывания своей облачной инфраструктуры, а так как РКН блокирует многие IP-адреса DigitalOcean, то доступ к некоторым ресурсам HTB может быть затруднен из нашей страны. Однако в данном случае в основном речь идет о веб-тасках раздела CTF, где уязвимые серверы «смотрят» напрямую в интернет, а не спрятаны за VPN, как основная лаборатория с виртуальными машинами.

Root Me

Root Me — еще одна уникальная площадка для практики пентеста и решения головоломок в духе CTF. Если снова взглянуть на наш список разновидностей ресурсов в начале статьи, то можно сказать, что эта платформа включает в себя первую область и своеобразную комбинацию двух последующих.

HOME / INFORMATION / THE PROJECT



Root-Me is a non-profit organization which goal is to promote the spread of knowledge related to hacking and information security.

This page is an introduction to the portal, its projects, his community but also to its philosophy. We encourage visitors to take an active part in the development of this community and its projects.

Community

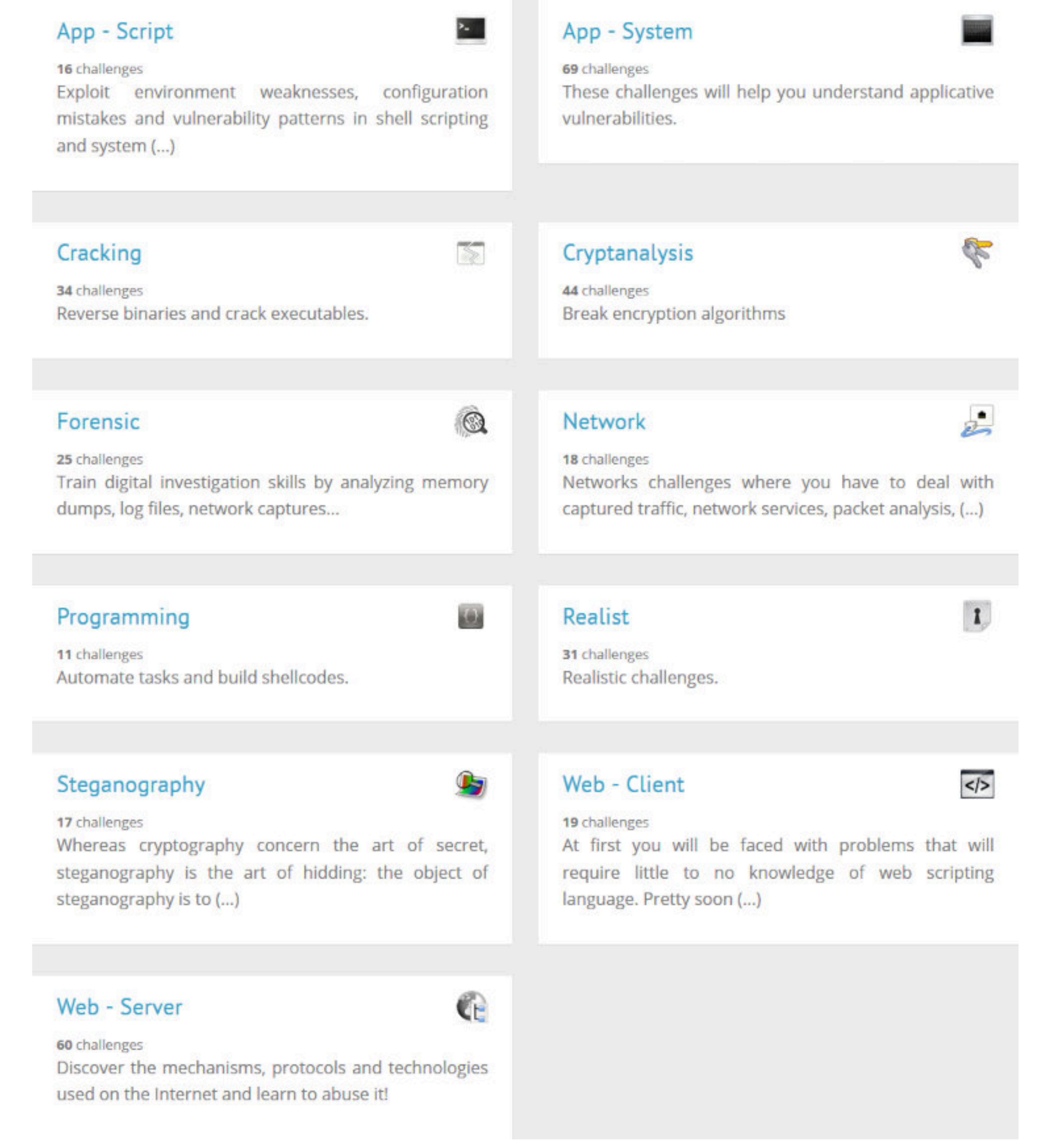
This association and its members are constituting a community where all the users can contribute and participate to the development of the website. We are a very open-minded organization that encourage an active participation, and we have set up various means to permit our users to get involved. We offer a publication system open to all permitting to post news, articles and other external resources to the website. We will try to maintain a relaxed atmosphere in order to allow everybody to learn and to participate in the best conditions. Here, the hierarchy doesn't exist, we are all equal before science.

Philosophy

We think that everybody must have a free access to every information. Hacking must not be a privilege. In this world where Internet growth with giant strides, everybody should be able to learn and to understand computer security. We offer you a free platform to allow you to train. It is therefore natural to ask some ethical questions. We consider hacking and its technique as a tool. It can be used beneficially (White-Hat) or harmfully and destructive (Black-Hat). We want to promote it as a weapon for social fight. Hacking is justified for fighting against oppression, inequality and censorship. Even if we don't encourage illegal IT acts, we want to promote and show you a positive alternative to the Black-Hat hacking. Join our community!

Root Me

Раздел с задачами CTF действительно внушительный: включает в себя 11 разделов с 344 тасками в целом.



CTF-таски — Root Me

Особенность многих из них заключается в том, что тебе нужно будет взаимодействовать с удаленным хостом, а не просто иметь дело с локальными файлами таска. Удобно, что для подключения можно использовать WebSSH прямо из браузера.



Сессия WebSSH из браузера Firefox

Однако главная фишка сайта — это раздел CTF all day: в этом режиме тебе доступен выбор из двадцати «комнат», каждая из которых активна в течении четырех часов. Присоединившись к любой из них, ты получишь краткую справку об объекте атаки и информацию о расположении флагов. Некоторые комнаты — это полноценные лаборатории со связкой из нескольких виртуальных машин с контроллером AD и общей легендой. Нужно сильно постараться, чтобы одолеть такие комнаты.

20 Available rooms

Room	Virtual machine chosen by players	State
ctf01	BBQ Factory	**running** *Time remaining : 07:13:47*
ctf02	Kioptrix level 2	**running** *Time remaining : 00:07:50*
ctf03	Awky	**running** *Time remaining : 00:26:19*
ctf04	LAMP security CTF5	**running** *Time remaining : 01:46:37*
ctf05	Hopital Bozobe	**running** *Time remaining : 00:32:28*
ctf06	Bluebox 2 - Pentest	**running** *Time remaining : 01:36:06*
ctf07	Bluebox - Microsoft Pentest	**running** *Time remaining : 01:18:49*
ctf08	Django unchained	**running** *Time remaining : 02:57:46*
ctf09	Django unchained	**running** *Time remaining : 03:54:41*
ctf10	/dev/random : Pipe	**running** *Time remaining : 04:37:37*
ctf11	None	**waiting**
ctf12	SSRF Box	**running** *Time remaining : 03:57:58*
ctf13	None	**waiting**
ctf14	None	**waiting**
ctf15	None	**waiting**
ctf16	BBQ Factory	**running** *Time remaining : 01:16:53*
ctf17	Sambox v4	**running** *Time remaining : 03:23:05*
ctf18	None	**waiting**
ctf19	Sambox v4	**running** *Time remaining : 00:37:44*
ctf20	None	**waiting**

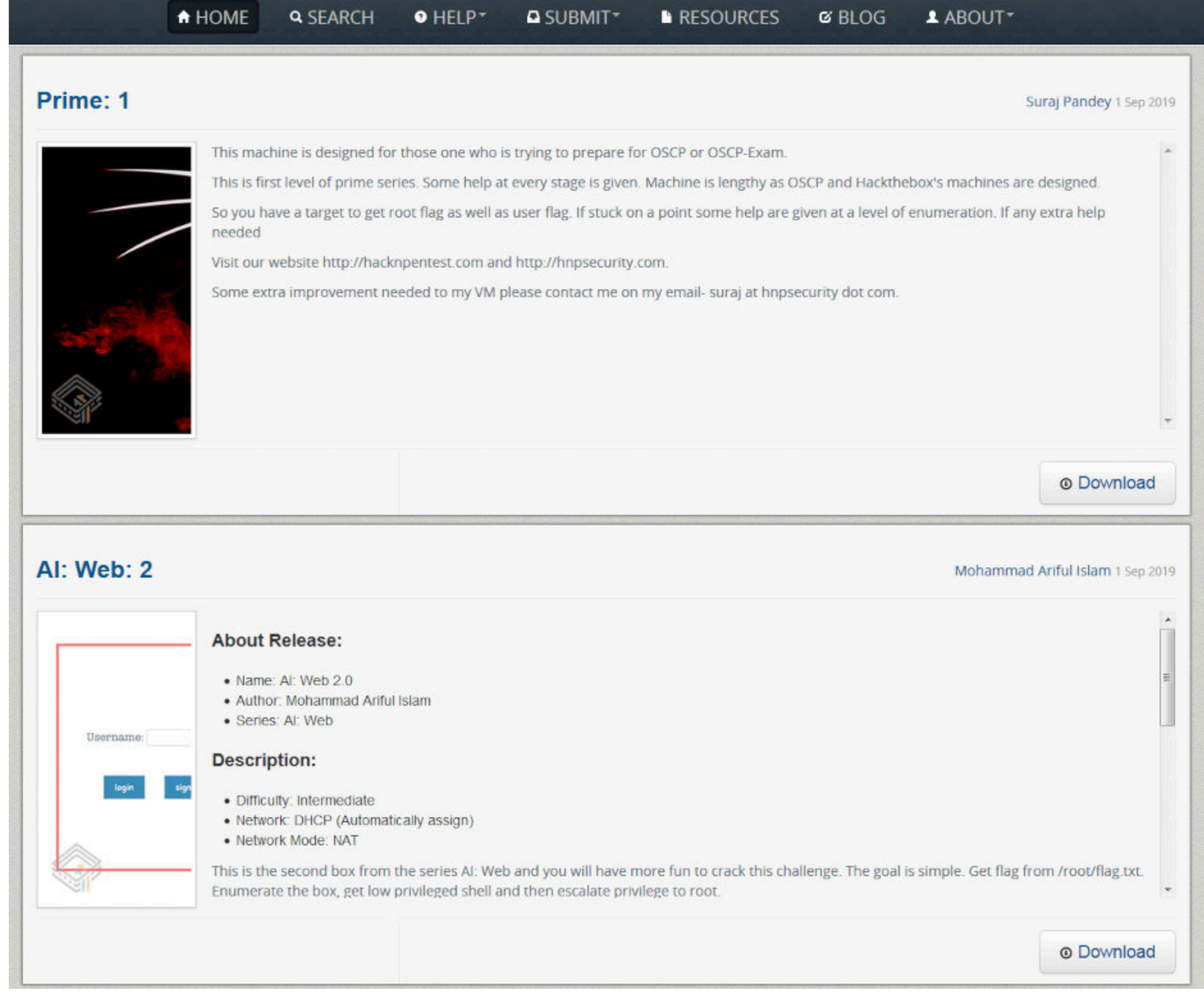
CTF all day — 20 активных комнат

Что касается общего уровня сложности, то, по моему мнению, он несколько ниже, чем у

Hack The Box. Несмотря на это, большее разнообразие CTF-тасков и возможность потренироваться на более лайтовых полигонах с Active Directory ставят площадку Root Me в список «маст хэв» ресурсов для практики пентеста.

VulnHub

VulnHub — старинный дамп образов уязвимых виртуальных машин, поддерживаемый энтузиастами. Это полностью бесплатный источник, откуда любой желающий может загрузить понравившуюся ему виртуалку и приступить к поиску флагов.



VulnHub

Одно из самых крупных преимуществ VulnHub — огромное количество райтапов по виртуалкам, доступных в сети, и отсутствие каких-либо ограничений на их публикацию (Hack The Box и Root Me накладывают временные рамки, в течении которых действует запрет на размещение прохождений в сети — в противном случае есть риск схватить бан, если публикуешься под своим никнеймом).

Большой выбор машин и райтапов делают VulnHub отличной отправной точкой для людей, которые совсем не знают, с чего начать свои эксперименты в области пентеста.

Из минусов:

- Часто к машинам нет внятного описания, которое позволило бы понять, что собой представляет машина. Так как все разнообразие существующих на VulnHub машин можно грубо разделить на две категории (с направленностью в жанр Task Based CTF и более приближенные к реальной жизни виртуалки), то каждый раз, загружая новый образ, в сущности, ты берешь кота в мешке и не знаешь, с задачей какого типа тебе предстоит столкнуться.
- Тотальное отсутствие машин на Windows. Ну оно и понятно — все же опенсорсный ресурс.

В остальном VulnHub — это прекрасный способ убить вечер с пользой и «поиграть» с интересными образами, собранными безопасниками для безопасников.



WWW

Полный список доступных на VulnHub вируталок можно найти по ссылке.

Рекомендации для начинающих

В тезисах постараюсь изложить основные моменты, которые обязательно пригодятся тем, кто планирует начать работу с каким-либо из вышеописанных ресурсов.

Для начала — про настройку окружения.

1. Средства виртуализации — твои друзья. Выбери из решений для работы с образами виртуальных машинам (ViruaIBox или VMware для Windows, KVM для Linux) и придерживайся его. Умение быстро разворачивать гостевые ОС пригодится не только в сфере безопасности.
2. Дистрибутивы, ориентированные на проведение пентестов — это круто. Kali

Linux, Parrot OS, BlackArch Linux, Commando VM, — неважно, что ты выберешь, главное, что они удобны для установки и практичны в использовании (на начальных этапах я бы остановился на Kali или Parrot). Независимо от того, что ты решил установить — устанавливай также строго в качестве виртуальной машины: таким образом ты уменьшишь риски нежелательных воздействий со стороны других, возможно, менее этичных хакеров, если планируешь подключаться к онлайновым лабораториям (то есть выделенным виртуальным сетям) по VPN.
3. Изучи консоль и сократи использование графического интерфейса ОС — это полезный навык практически для любой области IT. Работая в командной строке, ты значительно увеличишь свою производительность, научишься лучше концентрироваться на текущей проблеме (а не на переключении между открытыми окнами) и не будешь беспомощен, когда графического интерфейса не будет под рукой в принципе. В этом же пункте настоятельно рекомендую научиться обращению с каким-либо терминальным мультиплексором (я предпочитаю tmux, хотя уверен, что многие не сойдутся со мной в этом выборе), чтобы не переключаться между вкладками в окне эмулятора терминала.

Теперь непосредственно про процесс исследования уязвимых виртуальных машин.

1. «Enumeration is the Key» — самый частый ответ наряду с «Try Harder!» на крики о помощи на всевозможных форумах. Начальный сбор информации об объекте атаки — пожалуй, самый кропотливый этап всей кампании, а иногда и самый трудоемкий. Чем больше начальных данных, тем больше материала для анализа, тем больше поверхность возможных атак. Всегда оставляй какую-либо разведывательную утилиту работать в фоне для проверки очередного вектора проникновения.
2. Знай свои инструменты. Умение применить нужный софт в нужной ситуации — половина успеха операции. В сети существует множество списков полезных тулз для взлома, однако эти списки ничего не стоят, если никогда не пробовал инструмент «вживую». Поэтому, работая с чем-то новым, не пренебрегай командой `man` и опцией `--help` для получения базового представления о возможностях программы.
3. Не стесняйся искать информацию в сети, «гуглить — не стыдно!». Сфера компьютерной безопасности колоссально велика, очень трудно объять ее целиком, да и не всегда это нужно, если можно что-то быстро найти на просторах интернета. Это не то же самое, что быть скрипт-кидди — до тех

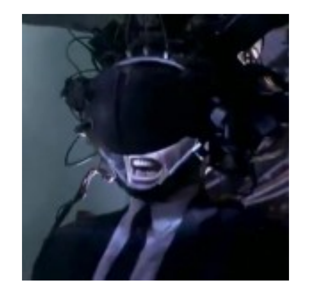
пор, пока можешь внятно объяснить, как ты добился того или иного результата (с техническими подробностями), волноваться не о чем.
4. Читай блоги и райтапы своих коллег — даже если ты уже одолел какую-то машину. Взгляд на одну и ту же проблему под разными углами способствует расширению рамок мышления и накоплению разностороннего опыта решения однотипных задач. Это может оказаться весьма полезным в условиях ограниченных ресурсов (сработает не одно, так другое).
5. Не ленись вести заметки — как непосредственно в процессе пентеста для поддержания организованности работы (здесь может помочь CherryTree или KeepNote), так и после успешного завершения взлома для систематизации полученных знаний. Отличным вариантом может стать написание райтапа к побежденной машине, потому что в процессе объяснения своего прохождения другим, ты дополнительный раз закрепляешь усвоенную информация.

Happy hacking!



WWW

Бонус: легендарный хакерский форум Antichat недавно запустил свою CTF-площадку. Самому пока не удалось испробовать, но не смог не включить это в статью.



snovvcrash

Безопасник, временами питонщик, местами криптоана(рхист)литик, по необходимости системный администратор. Люблю котов, неоновый свет, киберпанк, пси-транс и зелёные буквы на чёрных фонах терминальных эмуляторов.



Теги: CTF White hat Взлом Выбор редактора Пентестинг Статьи